UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,424	06/24/2003	Branislav N. Meandzija	15685P208	3310

45222 7590 03/18/2008

ARRAYCOMM/BLAKELY
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
03/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,424	MEANDZIJA ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2007(RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,8,9,17-19,21,24,33-35,37 and 40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5, 8, 9, 17-19, 21, 24, 33-35, 37, 40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's submission for RCE filed on Dec. 20, 2007 has been entered. Claims 1-3, 5, 8, 9, 17-19, 21, 24, 33-35, 37, 40 are pending.

Claim Objections

2. Claims 37, 40 are objected to because of the following informalities:

Claims 37, 40 depend on the cancelled claim 36, 39 respectively, which are treated as typographical error. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. Claims 8, 24 and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 8, 24 and 40, recite "wherein *the time parameter*", it is not clear which time parameter as claimed in claims 1, 17, 33 refers to.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 5, 9, 17, 21, 33 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer (Us Patent 6,009,173) in view of Kaliski Jr. (US patent 6,189,098) and in view of Ohno (US Patent No. 5,355,413).

As per claims 1, 17 and 33, Summer teaches a method, a user terminal and a machine-readable medium performed by a user terminal of a wireless access network, the method comprising: generating a shared secret to be provided to an access point of the wireless access network [Fig. 3, step 108, where sender-receiver session key is disclosed, see also col. 3, lines 32-34]; encrypting the shared secret with an access point public key [col. 3, lines 34-45, where the session key is encrypted using receiver's public key]; sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate, and the signed authenticator message [col. 3, lines 33-52];

Summer teaches generating an authenticator message and signing the authenticator message with the user terminal private key [col. 3, lines 26-28].

Summer doesn't expressively mention authenticator string including a portion of the shared secret.

However, Kaliski teaches the authenticator string including a portion of the shared secret [col. 4, lines 39-51, i.e. (KSS||TS) PUBserver and (CERT-C)KSS].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kaliski with Summer, since one would have been motivated to provide safeguard s against a third party impersonating the user terminal by simply replaying copies of the previous signatures intercepted or acquired [Kaliski, Jr., col. 1, lines 30-42].

Summer and Kaliski do not expressively mention pre-calculating a plurality of authenticator message based on a corresponding plurality of estimated time parameters; selecting a pre-calculated authenticator message that corresponds to the actual time parameter.

Ohno teaches pre-calculating a plurality of authenticator message based on a corresponding plurality of estimated time parameters; receiving an indication of an actual time parameter; and selecting a pre-calculated authenticator message that corresponds to the actual time parameter [Fig. 3, 4, col. 4 lines 55-64, col. 6 lines 27-37].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Ohno with Summer and Kaliski, since one would have been motivated to provide am authentication method which does not allow the fraudulent user to know the information regard to authentication code [Ohno, col. 1 lines 47-50].

As per claims 5, 21 and 37, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively, wherein signing the authenticator message comprises: generating a digest of the authenticator message (Summer, col. 3, lines 24-26); and encrypting the authenticator message digest with the user terminal private key (Summer, col. 3, lines 26-28).

As per claims 9, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claim 1, wherein the user terminal generates and encrypts the shared secret prior to identifying the access point by encrypting the shared secret with the public keys of a plurality of access points stored in the user terminal [Summer, col. 3 lines 34-35].

5. Claims 2, 3, 18, 19, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer (Us Patent 6,009,173) in view of Kaliski Jr. (US patent 6,189,098) Ohno (US Patent No. 5,355,413) and in view of Persson et al. (US Patent 6,754,824).

As per claims 2, 18 and 34, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claims 1, 17 and 33 respectively, except wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by both the transmitting node and the receiving node initializing a LFSR register by a common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secrete (Persson, col. 2, lines 5-23).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the method and system of Summer, Kaliski and Ohno for combining Persson's certificate with a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if week encryption or no encryption is switched on after authentication (Persson, col. 1, lines 35-49).

As per claims 3, 19 and 35, once modified, Summer teaches the method, the user terminal and the machine-readable medium of claims 2, 18 and 34 respectively, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point (Kaliski, Jr., col. 4, lines 42-55, i.e. KSS is used for symmetric key cryptography, the remainder of KSS||TS).

6. Claims 8, 24 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Summer (US Patent 6,009,173) in view of Kaliski Jr. (US Patent 6,189,098) Ohno (US Patent No. 5,355,413) and in view of Thompson, III et al. (US Pub. No. 2004/0131014).

As per claims 8, 24, and 40, Summer and Kaliski teach the method, the user terminal and the machine-readable medium of claims 1, 17 and 33 respectively, except the time parameter comprises an absolute frame number.

Thompson teaches calculating the authenticator message based on an absolute frame number [paragraph 0096].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Thompson with Summer, Kaliski and Ohno, since one would have been motivated to schedule the transmission of the data stream [Thompson, paragraph 0001, lines 3-4].

Response to Amendment

7. Applicant's submission for RCE filed on Dec. 20, 2007 has been entered. However, upon further consideration, a new reference by Ohno (US 5,355,413) is found and used in combination with various previously cited prior art. See new grounds of rejection above.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Deo et al (US 2002/0049905) – System for broadcasting to and programming a mobile device in protocol

Brainard et al (US 2003/0105964) – Method and Apparatus for performing enhanced time-based authentication

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP

3/10/08 ***/KIMYEN VU/***

Supervisory Patent Examiner, Art Unit 2135